

Master Innovation & Development Plan

Technical Appendix

**TITLE: An Update on Data Governance
for Sidewalk Toronto**

AUTHOR: Alyssa Harvey Dawson

ABSTRACT

Sidewalk believes Quayside can set a new model for responsible data use in cities —anchored by an independent Civic Data Trust.

Most relevant sections: Vol 2 (Digital Innovation)



An Update on Data Governance for Sidewalk Toronto

We believe Quayside can set a new model for responsible data use in cities—anchored by an independent Civic Data Trust.



Alyssa Harvey Dawson

Oct 15, 2018 · 6 min read

From its creation, Sidewalk Labs has recognized that digital tools have a big role to play—alongside great urban design and innovative policy—in tackling big urban challenges and improving quality of life in cities. The launch of Sidewalk Toronto sparked an active and healthy public discussion about data privacy, ownership, and governance.

Sidewalk Labs takes these issues seriously, and thanks everyone who has spoken up.

On Thursday, we will be presenting some initial proposals on digital governance in Quayside to Waterfront Toronto's Digital Strategy Advisory Panel. We're excited to get their feedback—and wanted to share our presentation with you. **You can find it [here](#).**

We hope you'll read the whole thing, but we realize it's long and complicated! So here is a quick summary of what we are proposing:

- No one has a right to own information collected from Quayside's physical environment—including Sidewalk Labs. Instead, this "urban data" should be under the control of an independent Civic Data Trust.
- To protect privacy, all entities proposing to collect or use urban data (including Sidewalk Labs) will have to file a Responsible Data Impact Assessment with the Data Trust that is publicly available and reviewable.
- With regard to the use of data, one set of rules will apply to everyone. Sidewalk Labs will not receive any special treatment.
- Sidewalk Labs will use open standards for any digital infrastructure and services it provides—so anyone can plug in or compete.

None of the ideas we're presenting are fixed or final. They are, however, consistent with our longstanding goal of setting a new standard for responsible data use that protects personal privacy and the public interest while enabling companies, researchers, innovators, governments, and civic organizations to improve urban life using urban data.

No one should own urban data—it should be made freely and publicly available.

Torontonians are concerned about data gathered in public places, even if that data is de-identified (wiped of personal info) or aggregated. For clarity, we call the original information collected in a physical place in the city "urban data." Urban data is different from data created when individuals agree to provide information through a website, mobile phone, or paper document. It presents unique challenges, including that it could reasonably be considered a public asset, and that it raises potential concerns around surveillance and privacy.

We believe all data needs protection, but the extent to which urban data specifically may be collected in Quayside is what's new and different here. Existing laws on urban data do not address ownership. And urban data is only regulated when it contains personally identifiable information. Even then, these rules are often not followed in the public realm. We seek to build on them.

We believe that, as a default matter, de-identified urban data should be made freely and publicly available. In these cases, there wouldn't be ownership of the data itself, or monetary value attached to it—everyone would have equal access. But value could be created when people or companies use urban data to improve city life with, say, a new navigation app, a smarter traffic light, an energy saver tool, or other digital services we can't imagine yet.

An independent Civic Data Trust should control urban data in Quayside.

If no one owns urban data, the question remains: Who manages it in the public interest?

Sidewalk Labs believes an independent Civic Data Trust should become the steward of urban data collected in the physical environment. This Trust would approve and control the collection of, and manage access to, urban data originating in Quayside. The Civic Data Trust would be guided by a charter ensuring that urban data is collected and used in a way that is beneficial to the community, protects privacy, and spurs innovation and investment.

We think the Civic Data Trust should make de-identified data freely and publicly available and maintain a public registry (online and easily searchable) of all devices that collect urban data. Approval from the Trust should be required to collect or use urban data on a more proprietary or commercial basis, or urban data that involves identifiable information.

Anyone seeking to collect urban data will need to demonstrate they're putting privacy—and the public interest—first through a Responsible Data Impact Assessment submitted to the Data Trust.

One of the strongest existing tools for protecting individual privacy is called a “privacy impact assessment.” These assessments are already supported by governments in Canada, and are also a cornerstone of GDPR, Europe’s newly implemented privacy legislation.

We want to build on these ideas with a Responsible Data Impact Assessment (RDIA)—an in-depth review and analysis triggered any time there is a proposal to collect or use urban data. RDIA’s will describe the **purpose** of a given proposal, the **sources of data** it requires, the potential **impact** on individuals or a community, and an **analysis** of its benefits and risks.

RDIA’s would have to be filed with the Civic Data Trust *before* the collection of urban data takes place, and they would be made publicly available—to create transparency and help hold companies and agencies accountable.

Simply put, RDIA’s help ensure that no entity collects urban data just for data’s sake. It must have a beneficial public purpose. They also help put into practice the critical Responsible Data Use principles we set forth in May, including the use of Privacy by Design, the need for clear and transparent signage when urban data is collected in public spaces, and the need for urban data to be de-identified by default.

No single entity—including Sidewalk Labs—should have special treatment when it comes to urban data. Urban digital systems should be open to all.

In Quayside, Sidewalk Labs expects to provide baseline digital infrastructure, such as internet connectivity, to make it easier for residents, companies, organizations, and local agencies to launch new services that improve urban life. But the fact that Sidewalk Labs plans to build these components does not preclude others from deploying technology that improves on, competes with, or replaces them.

And while Sidewalk Labs plans to develop a number of innovations—such as canopies that retract in advance of a storm, or buildings that prioritize clean energy—we expect the lion’s share of technologies that make Quayside unique to be developed and deployed by an ecosystem of many innovators.

To catalyze urban innovation in Quayside, Sidewalk Labs will use open standards in our technology and collaborate to define those standards with others working on urban innovation. Just as anyone can create a new website as long as they follow open standards, Quayside's open standards will promote collaboration and competition, prevent vendor lock-in, and inspire the new urban tools we expect to emerge along the waterfront.

Data protection is paramount—but it can be achieved without requiring data residency.

Sidewalk Toronto has been part of an active discussion about the rules related to “data residency,” or the physical location where urban data is stored. Many Torontonians have raised understandable concerns about whether the laws of Canada will apply to data potentially being stored outside the country.

But data localization presents a number of challenges, including that it runs counter to the way information travels across the internet and creates higher barriers to entry for startups. With specific exceptions, data localization is not presently a requirement of Canadian or Ontario law.

In line with other groups, including the Business Council of Canada, Sidewalk Labs believes that the goal of Canadian legal protection can be best achieved in other ways, including contractual requirements (such as agreements with cloud providers to handle data that originates in Canada in accordance with Canadian laws) and technical mechanisms (such as encryption, so data cannot be accessed no matter where it travels).

These ideas are still just the start.

What we are presenting to Waterfront Toronto will continue to evolve as we work toward publishing a draft of our Master Innovation and Development Plan for Sidewalk Toronto in early 2019. At that time, it will fall to government to assess our proposals and decide whether they have merit.

As the full presentation makes clear, a number of important questions still need to be answered, including: How should a Civic Data Trust be established? Should the Civic Data Trust act as a repository for data?

How will ongoing operations of the Civic Data Trust be funded? How can Sidewalk Labs best encourage use of open standards by others?

We think these ideas should be taken up in dedicated consultations with the public and experts. We've got some work to do to plan those consultations and will share details with you as soon as we have them.

In the meantime, we would welcome any thoughts you have—please email privacy@sidewalktoronto.ca. Let the conversation continue.

Follow what Sidewalk Labs is thinking, doing, and reading with our weekly [newsletter](#), or on [Twitter](#) and [Facebook](#).